Cassandra Crossing/ Find My ... Apple? Ma anche no

(506) . Un necessario ripasso di cosa succede, e succederà, quando tenete l'iPhone in tasca, anche spento.

Cassandra Crossing/ Find My ... Apple? Ma anche no

Figure 1:

(506) Un necessario ripasso di cosa succede, e succederà, quando tenete l'iPhone in tasca, anche spento.

6 giugno 2022—Cassandra si sente sempre spiazzata quando le sue profezie si avverano con più forza delle sue già molto fosche previsioni.

Le è appunto successo di recente, leggendo l'ottima descrizione tecnica della nuova versione della funzionalità "**Find my...**" nella prossima release di iOS.

Disclaimer: Cassandra ritiene necessario ricordare qui i suoi lontani trascorsi nel Lato Oscuro della Forza come "*Darth Calamari*", che in tempi remoti hanno incluso, e non solo, quelli di sviluppatore e di entusiasta Apple.

Poi un po' di saggezza le è entrata in testa, ed ha cominciato a vedere le cose importanti, come i "walled garden" il "customer lock-in" ed altri comportamenti di cui, va detto, l'azienda una volta in Mariani avenue, Cupertino, non ha assolutamente il monopolio, ma ne è solo il più grande campione. Si è proprio così; l'uomo noto oggi come "Cassandra" si è riunito al lato giusto della Forza, proprio come Anakin, e da allora non ha più sgarrato.

Ma oggi ci occuperemo di funzionalità interessanti ed utili di iOS, sperando di non cadere in imprecisioni, ma principalmente rovesciando la medaglia per vedere cosa c'è dietro.

“**Find my…**” unifica a livello interfaccia utente diverse funzioni e servizi posizionali già esistenti da tempo, e ne introduce altri.

E’ possibile localizzare il proprio computer o telefono, se “Find My…” è abilitato sul dispositivo, come pure avere la posizione degli eventuali AirTag posseduti. Si possono avere allarmi se un dispositivo viene spento, oppure se viene riacceso, magari dopo un furto, oppure se ci si allontana oltre una certa distanza da un dispositivo.

Il proprietario stesso viene “parificato” ad un dispositivo, e nelle localizzazioni possono essere integrati i propri amici “consenzienti”, ed è possibile una vista complessiva della propria famiglia e dei relativi dispositivi.

Si tratta certamente di funzioni utili, e ben integrate nel sistema operativo e nei dispositivi, cosa certo più facile per Apple che per la concorrenza, visto che Apple deve essere compatibile solo con sé stessa.

Ma tutte queste funzionalità, nella cui descrizione ci saranno state certamente omissioni ed imprecisioni, non sono interesse di Cassandra; il “come” queste funzionalità sono realizzate è la cosa più importante.

Infatti, limitandoci al caso degli smartphone e non considerando tutte le altre tipologie di dispositivi Apple, secondo la descrizione di questa funzionalità, “**Find My…**” può trovare un telefono che è:

- spento;
- con la batteria scarica;
- che è stato formattato e riportato alla configurazione di fabbrica.

Ora, la domanda che Cassandra si pone non è “come funziona” ma piuttosto “come è possibile che funzioni”. Le risposte sono (quasi) tutte nell’articolo suddetto o nella insoddisfacente documentazione tecnica ufficiale.

Un iPhone, come praticamente tutti gli smartphone moderni, ha un GPS incorporato per rilevare direttamente la propria posizione, e 4 o 5 connessioni wireless:

- GSM, la connessione normalmente che si utilizza per telefonare;
- WIFi, la connessione normalmente usata per connettersi ad Internet;
- Bluetooth, la connessione normalmente usata per connettersi agli auricolari, all’auto o ad altri dispositivi Bluetooth molto vicini;
- NFC, la connessione per comunicare con carte di credito, lettori di badge ed altro;
- UWB, il protocollo radio Ultra-Wideband, realizzato dal chip U1;

Il chip U1, di cui i prodotti Apple più recenti (a partire dall’iPhone 11) sono dotati, come ad esempio gli Airtag, è qui di particolare interesse.

Ora, nessun problema esiste ovviamente per tracciare un dispositivo che “conosce” la propria posizione se questo è in grado di connettersi via GSM o WiFi.

Ma se il telefono non ha la SIM o questa è scaduta, e se non ci sono reti WiFi a cui ci si possa connettere, come è possibile che la funzionalità Find My possa operare, ad esempio per rintracciare un dispositivo perduto o rubato.

In termini semplici, i dispositivi Apple formano una rete di tipo “mesh”, collegandosi automaticamente ed in maniera trasparente ad ogni altro dispositivo Apple che sia raggiungibile via Bluetooth, cioè che si trovi ad una distanza dell’ordine dei 10 metri. Questo pare possa avvenire anche via UWB.

Utilizzando accorgimenti che cercano di “tutelare la privacy” del possessore del dispositivo, tutti i dispositivi circostanti “inoltrano” ad un cloud centrale proprietario Apple l’indirizzo e la posizione del dispositivo perso, che non ha di per sé la possibilità di collegarsi via GSM o WiFi, e magari non conosce nemmeno la propria posizione.
In questo modo, tramite il proprio account iCloud, il proprietario può conoscere, con un certo grado di approssimazione, la posizione del dispositivo perduto.

Ed ora veniamo a quello che Montalbano chiamerebbe “*Il carrico da undici*”.

Come viene tracciato un device spento?

Beh, in fondo è semplice, come tanti altri apparecchi moderni e “ripieni” di software, ad esempio smart-TV od autoveicoli, viene tracciato perché non è “completamente” spento.

Uno o più dei chip U1, Bluetooth od NFC è alimentato, ed un programma, eseguito non sulla cpu principale del telefono (per motivi di consumo, è in grado di comunicare via radio.

E se il dispositivo ha addirittura la batteria scarica?

Quando la batteria si scarica, il dispositivo Apple continua ad inviare sulla rete mesh la propria posizione, anche per un certo tempo dopo che la batteria è troppo scarica per alimentare l’intero telefono, ma le resta comunque abbastanza energia da poter continuare ad alimentare il chip che provvede a comunicare con i dispositivi vicini. Infine un attimo prima di spegnersi davvero completamente invia un’ultima volta la sua posizione.

Insomma, riassumendo:

I dispositivi Apple comunicano su una rete mesh proprietaria, che non è conosciuta dalla stragrande maggioranza di utenti e non è documentata a livello utente, e lo è poco a livello sviluppatori.

I dispositivi Apple fanno molte “cose” anche quando il proprietario pensa di averli spenti.

I dispositivi Apple, entro certi limiti, fanno alcune “cose” anche con la batteria quasi completamente scarica.

Tutto questo può anche essere giudicato una caratteristica positiva dei dispositivi Apple; permette di avere funzionalità molto interessanti ed utili, ed in certi casi di contrastare “cattivi”.

Ma per voi è confortevole vivere con un dispositivo che non può essere spento e che comunica permanentemente con altri?

Ecco, qui possiamo tranquillamente (“tranquillamente” ???) generalizzare il discorso all’intero mercato IoT, senza continuare a gettare la croce addosso solo ai proprietari di dispositivi Apple, visto che queste “funzionalità” potrebbero tranquillamente esistere già non solo sugli smartphone Android, ma anche in quasi tutti gli oggetti IoT di ultima generazione.

E’ un ragionamento per poveri paranoici pretendere di sapere, in maniera semplice ed evidente, cosa fa un oggetto appena acquistato, ed essere sicuri di poterlo disattivare o spegnere completamente senza doverlo tritare?

Cassandra pensa che dovrebbe addirittura essere indicato sulla scatola, con quelle icone standard che sono tanto utili.

Ogni lettore avrà certamente la sua risposta.

E se qualcuno pensasse che il “tritare i dispositivi” per renderli sicuri sia una boutade di Cassandra, controlli le prescrizioni di smaltimento dei dispositivi che contengono od hanno contenuto dati top-secret.

In tutti i paesi che ne hanno pubblicato delle specifiche tecniche, o in cui questa sono state leakate, queste prevedono la distruzione fisica completa (sminuzzamento, dissoluzione con acidi o polverizzazione) dei dispositivi a stato solido che hanno contenuto dati top secret, ad esempio laptop e smartphone.

Ne sa qualcosa un primo ministro inglese che, avendo improvvidamente collegato, per caricarlo, il cellulare personale ad un laptop top secret, si è visto sequestrare e tritare il cellulare dai servizi segreti.

Ed ecco ad esempio, un video su quello che i servizi segreti inglesi hanno preteso dovesse essere fatto dai giornalisti di "The Guardian" per distruggere un computer che aveva contenuto dei dati (per gli inglesi, e non solo per loro, top secret) forniti da Edward Snowden.

Ma torniamo a noi, questa puntata si conclude qui, di colpo e semplicemente con una domanda.

A Lovercraft le cose che sussurravano nel buio in fondo piacevano, ma voi, **voi volete oggetti come questi in tasca o dentro casa**?

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on June 7, 2022.

Canonical link

Exported from Medium on August 27, 2025.